http://dx.doi.org/10.35596/1729-7648-2019-124-6-80-86

Оригинальная статья
Original paper

УДК 004.75

МОНИТОРИНГ ТЕХНОГЕННЫХ ОБЪЕКТОВ, ДОСТУПНЫХ ИЗ СЕТИ ИНТЕРНЕТ

СМОЛЯК Д.С., ПЕТРОВ С.Н., ПУЛКО Т.А.

Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь

Поступила в редакцию 11 марта 2019

Аннотация. Исследована возможность обнаружения и мониторинга техногенных объектов Республики Беларусь, доступных из сети Интернет. Предложен метод обнаружения, основанный на анализе данных публичных сервисов Shodan и Censys. Разработано программное обеспечение, позволяющее автоматизировать мониторинг.

Ключевые слова: автоматизированная система управления технологическим процессом, Интернет вещей, мониторинг, информационная безопасность.

Конфликт интересов. Авторы заявляют об отсутствии конфликта интересов.

Для цитирования. Смоляк Д.С., Петров С.Н., Пулко Т.А. Мониторинг техногенных объектов, доступных из сети Интернет. Доклады БГУИР. 2019; 6(124): 80-86.

MONITORING OF INTERNET-FACING TECHNOGENIC OBJECTS

SMOLIAK D.S., PETROV S.N., PULKO T.A.

Belarusian State University of Informatics and Radioelectronics, Republic of Belarus

Submitted 11 March 2019

Abstract. The approach to detection and monitoring of Internet-facing technogenic objects has been described. The method of analysis of public services Shodan and Censys has been proposed. The automation monitoring software has been developed.

Keywords: supervisory control and data acquisition, Internet of Things, monitoring, information security.

Conflict of interests. The authors declare no conflict of interests.

For citation. Smoliak D.S., Petrov S.N., Pulko T.A. Monitoring of Internet-facing technogenic objects. Doklady BGUIR. 2019; 6(124): 80-86.

Введение

Информационные системы техногенных объектов содержат элементы традиционных информационных систем, такие как серверы приложений, базы данных, сетевые устройства, и специфические элементы, относящиеся к промышленных сетям, программируемые логические контроллеры (Programmable Logic Controller, PLC), распределенные системы управления (Distributed Control System, DCS), системы управления зданиями (building management systems, BMS). Повышение сложности системы увеличивает риски возникновения ошибок и, как следствие, компрометации информационной системы. В случае с техногенными объектами последствия компрометации могут быть катастрофическими. Одним из векторов компрометации информационных систем является небезопасная настройка. Умышленные и случайные ошибки в настройке средств защиты информации и прикладного программного обеспечения могут привести к тому, что элементы информационных систем техногенных объектов станут доступны из сети Интернет.

В данной статье предложен метод обнаружения элементов промышленных сетей техногенных объектов Республики Беларусь, доступных из сети Интернет, основанный на анализе открытых данных, содержащих результаты сканирования всего диапазона адресов протокола IP версии 4. Авторами разработано программное обеспечение, позволяющее автоматизировать поисковые запросы и агрегировать их результаты, что дает возможность своевременно обнаружить доступные из сети Интернет устройства и принять меры по снижению или устранению рисков компрометации информационной системы техногенного объекта.

Теоретический анализ

Вопросы информационной безопасности техногенных объектов являются критически важными для государств ввиду тяжести возможных последствий от успешной реализации угроз информационной безопасности. В качестве примера можно привести взлом системы управления водоснабжением США, произошедший в 2011 году [1]. Данной атакой были затронуты программируемые логические контроллеры, управляющие водоснабжением. Также показательным примером является атака с помощью вредоносного программного обеспечения BlackEnergy на энергетическую систему Украины, результатом которой были сбои в электроснабжении отдельных населенных пунктов [2]. Таким образом, техногенные объекты требуют пристального внимания в отношении вопросов информационной безопасности.

В качестве мер по предупреждению инцидентов и повышению осведомленности государственные регуляторы в области информационной безопасности выпускают различные требования и рекомендации по обеспечению информационной безопасности критически важных объектов, к которым относятся техногенные объекты. В частности, Национальный институт стандартов и технологий США (The National Institute of Standards and Technology, NIST) в рамках серии публикаций, посвященных информационной безопасности, выпустил руководство по обеспечению безопасности промышленных систем управления [3]. Руководство содержит ряд мер, направленных на повышение защищенности промышленных систем управления. Одной из мер, рассматриваемой в политике межсетевого экранирования, является явный запрет на подключение промышленных сетей к сети Интернет.

Тем не менее из сети Интернет доступно огромное количество устройств, являющихся частью промышленных сетей предприятий, что ставит под угрозу безопасность информационных систем, частью которых они являются [4–6].

В связи с этим возникает необходимость в мониторинге и своевременном обнаружении доступных из сети Интернет промышленных устройств и принятию мер по предотвращению угроз, связанных с их возможной компрометацией.

Методы обнаружения промышленных устройств

Для того чтобы получить информацию о подключенных к сети Интернет устройствах, можно осуществить сканирование диапазона IP-адресов на наличие открытых портов, определить сервисы, работающие на открытых портах. Трудоемкость этой задачи зависит от диапазона сканируемых IP-адресов, и как следствие, большие диапазоны адресов требуют большого времени сканирования. Более эффективным методом является использование готовых результатов сканирования всего диапазона адресов протокола IP версии 4. Такие результаты предоставляют сервисы Shodan и Censys.

Сервисы Shodan и Censys агрегируют результаты сканирования и предоставляют доступ к ним с помощью поисковых запросов. Каждый из сервисов обладает собственным набором ключевых слов для осуществления поисковых запросов. Таким образом, для поиска одинаковой информации необходимо использовать уникальные для каждого сервиса поисковые запросы.

Сервис Shodan поддерживает полнотекстовый поиск, фильтры и метки. Полнотекстовый поиск позволяет получать результаты в случае отсутствия точных параметров запроса, фильтры позволяют задать точные параметры запроса, метки позволяют осуществлять поиск по заданным разработчиками категориям.

Для поиска промышленных устройств в сервисе Shodan авторы выделили следующие методы, представленные в табл. 1.

Таблица 1. Методы поиска в Shodan
Table 1. Search methods in Shodan

Метод поиска	Ключевые слова запроса	Примечания
Поиск по меткам	scada ics plc	
Поиск по номеру порта протокола промышленной сети	port:502 port:102 port:1911,4911 port:20000 port:47808 port:44818 port:18245,18246 port:5094 port:1962 port:5006,5007 port:9600 port:789 port:2455 port:2404 port:20547	протокол Modbus протокол Siemens S7 протокол Fox протокол DNP3 протокол BACNET протокол EtherNet/IP протокол GE-SRTP протокол HART IP протокол PCWorx протокол MELSEC-Q протокол FINS протокол Red Lion протокол CODESYS протокол IEC 60870-5-104 протокол ProConOS

Пример поискового запроса для протокола Modbus в сервисе Shodan представлен на рис. 1.

Сервис Censys, так же как и Shodan, поддерживает полнотекстовый поиск, фильтры и метки. Кроме того, поддерживаются логические операторы, такие как «AND», «OR». Для фильтрации выдачи можно перечислить порт, протокол, метод, диапазон IP-адресов, географическое положение или ограничения по дате. Censys осуществляет еженедельное сканирование всего диапазона адресов протокола IP версии 4 для промышленных протоколов Siemens S7, MODBUS, Niagara Fox, DNP3, BACnet.

Для поиска промышленных устройств в сервисе Censys авторы выделили следующие методы, представленные в табл. 2.

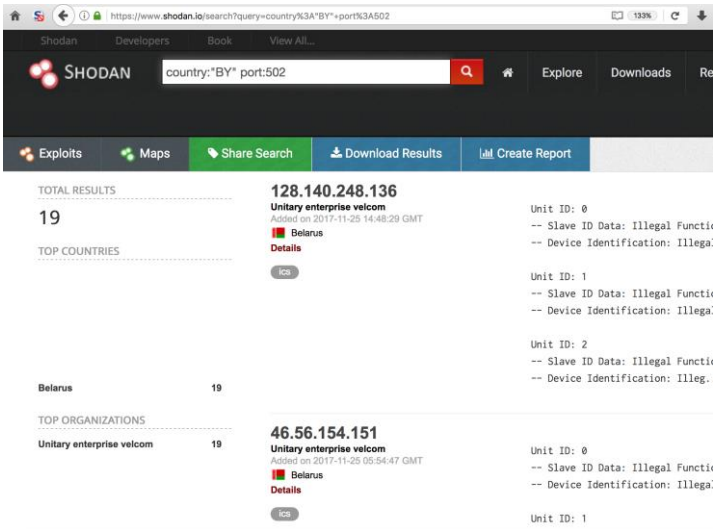

Рис. 1. Поисковой запрос Shodan – Modbus
Fig. 1. Search query Shodan – Modbus

Таблица 2. Методы поиска в Censys
Table 2. Censys Search Methods

Метод поиска	Ключевые слова запроса	Примечания
Поиск по меткам	scada scada server scada router building control modbus bacnet fox	
Поиск по номеру порта протокола промышленной сети	protocols:"502/modbus" protocols:"102/s7" protocols:"1911/fox" protocols:"20000/dnp3" protocols:"47808/bacnet"	протокол Modbus протокол Siemens S7 протокол Fox протокол DNP3 протокол BACNET

Пример поискового запроса для протокола Modbus в сервисе Censys представлен на рис. 2.

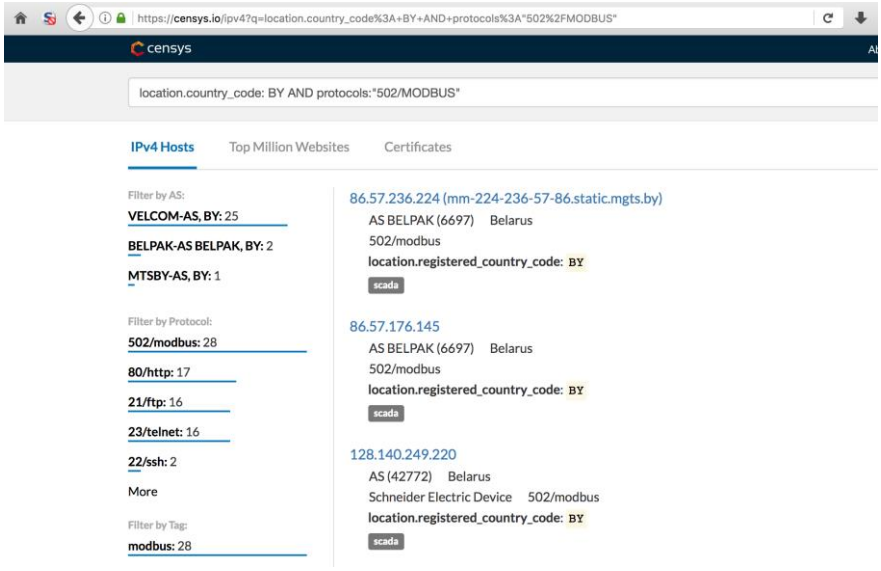

Рис. 2. Поисковой запрос Censys – Modbus
Fig. 2. Search query Censys – Modbus

Таким образом, сервисы Shodan и Censys могут быть использованы для получения информации о доступных из Интернет промышленных устройствах, являющихся частью информационных систем техногенных объектов.

Автоматизированный мониторинг промышленных устройств

Сервисы Shodan и Censys обладают интерфейсами прикладного программирования (Application Programming Interface, API). Это позволяет осуществлять поисковые запросы к сервисам из разработанных сторонними разработчиками приложений. Эта возможность использовалась авторами для создания программного обеспечения автоматизации мониторинга scadamonitor.py (рис. 3).

```
root@kali:~# scadamonitor.py --help
usage: scadamonitor.py [-h] [--country COUNTRY] [--tag TAG] [--engine ENGINE]
                       [--output OUTPUT] [--proto PROTO]

optional arguments:
  -h, --help         show this help message and exit
  --country COUNTRY  Select 2-digit country region. Default = "by"
  --tag TAG          Select search tag. Default = "scada"
  --engine ENGINE    Select search engine (shodan,censys,all). Default = "all"
  --output OUTPUT    Select output format (json, csv, screen, all). Default =
                     "screen"
  --proto PROTO      Select search protocols (S7, modbus, bacnet, fox, all).
                     Default = "all"
```

Рис. 3. Программное обеспечение scadamonitor.py
Fig. 3. Scadamonitor.ru software

Разработанное программное обеспечение scadamonitor.py позволяет автоматизировать поиск информации в сервисах Shodan и Censys, агрегировать результаты поиска, осуществлять экспорт результатов поиска в форматах CSV и JSON. В качестве языка программирования использовался Python ввиду удобства его использования.

Пример автоматизации поисковых запросов для IP-адресов, относящихся к диапазону Республики Беларусь, приведен на рис. 4.

```
root@kali:~# scadamonitor.py

=============== Task params ===============
Country: BY
Tags: scada
Engine: all
Output: screen
Protocols: all


=============== Shodan search started ===============
0 results found
=============== Shodan search finished ===============


=============== Censys search started ===============
37 results found

=============== Censys results ===============
86.57.236.224 - 502/modbus
37.17.110.182 - 102/s7
86.57.176.145 - 502/modbus
46.56.155.3 - 502/modbus
37.17.96.124 - 502/modbus
37.212.17.70 - 47808/bacnet
128.140.249.220 - 502/modbus
178.163.162.131 - 502/modbus
128.140.249.7 - 502/modbus
128.140.249.155 - 502/modbus
128.140.249.156 - 502/modbus
46.56.148.121 - 502/modbus
128.140.249.6 - 502/modbus
86.57.167.80 - 502/modbus
```

Рис. 4. Пример работы программного обеспечения мониторинга
Fig. 4. Example of monitoring software

Описание параметров, используемых программным обеспечением, приведено в табл. 3.

Таблица 3. Входные параметры scadamonitor.py
Table 3. Input parameters of scadamonitor.ru

Параметр	Значение	Значение по умолчанию	Описание
--help	–	–	получение справочной информации
--country	by	by	выбор географического диапазона IP-адресов
--tag	scada, ics, plc	scada	используемая метка поиска
--engine	shodan, censys, all	all	используемый сервис поиска, значение all означает поиск во всех сервисах
--output	json, csv, screen, all	screen	формат вывода результатов поиска, screen означает вывод результатов на экран, CSV – вывод в файл в формате CSV, JSON – вывод в файл в формате JSON
--proto	S7, modbus, bacnet, fox, all	all	поддерживаемые протоколы, значение all означает поиск по всем протоколам (s7, modbus, bacnet, fox)

Заключение

Рассмотрена возможность обнаружения техногенных объектов, доступных из сети Интернет. Проанализирована возможность использования общедоступных сервисов, содержащих информацию о результатах сканирования всего диапазона адресов протокола IP версии 4. В результате поиска обнаружены промышленные устройства, подключенные к сети Интернет. Разработано программное обеспечение, позволяющее осуществлять мониторинг в сервисах Shodan и Censys по ключевым словам и протоколам.

Список литературы / References

1. SCADA-based water system hacked [Electronic resource]. URL: https://www.scmagazineuk.com/scada-based-water-system-hacked/article/547552 (date of access: 11.02.2019).
2. Cyber-Attack Against Ukrainian Critical Infrastructure [Electronic resource]. URL: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01 (date of access: 11.01.2019).
3. Guide to Industrial Control Systems (ICS) Security [Electronic resource]. URL: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf (date of access: 12.01.2019).
4. Traffic light controls – Shodan finds the Internet's most dangerous spots [Electronic resource]. URL: http://money.cnn.com/gallery/technology/security/2013/05/01/shodan-most-dangerous-internet-searches/index.html (date of access: 11.01.2019).
5. Project SHINE: 1,000,000 Internet-Connected SCADA and ICS Systems and Counting [Electronic resource]. – URL: http://www.tofinosecurity.com/blog/project-shine-1000000-internet-connected-scada-and-ics-systems-and-counting (date of access: 11.01.2019).
6. SCADA cybersecurity in the age of the Internet of Things [Electronic resource]. URL: https://www.controleng.com/single-article/scada-cybersecurity-in-the-age-of-the-internet-of-things/94eccaddb83842690e375274395e629e.html (date of access: 21.01.2019).
7. Shodan [Electronic resource]. URL: https://www.shodan.io (date of access: 20.02.2019).
8. Censys [Electronic resource]. URL: https://censys.io (date of access: 20.02.2019).

Сведения об авторах

Смоляк Д.С., аспирант кафедры защиты информации Белорусского государственного университета информатики и радиоэлектроники.

Information about the authors

Smoliak D.S., postgraduate student of information security department of Belarusian State University of Informatics and Radioelectronics.

Петров С.Н., к.т.н., доцент, доцент кафедры защиты информации Белорусского государственного университета информатики и радиоэлектроники.

Пулко Т.А., к.т.н., доцент, доцент кафедры защиты информации Белорусского государственного университета информатики и радиоэлектроники.

Адрес для корреспонденции

220013, Республика Беларусь,
г. Минск, ул. П. Бровки, 6,
Белорусский государственный университет
информатики и радиоэлектроники
тел. +375-17-293-85-58;
e-mail: smoliakd@gmail.com
Смоляк Дмитрий Сергеевич

Petrov S.N., PhD, associate professor, associate professor of information security department of Belarusian State University of Informatics and Radioelectronics.

Pulko T.A., PhD, associate professor, associate professor of information security department of Belarusian State University of Informatics and Radioelectronics.

Address for correspondence

220013, Republic of Belarus,
Minsk, P. Brovka str., 6,
Belarusian State University
of Informatics and Radioelectronics
tel. +375-17-293-85-58;
e-mail: smoliakd@gmail.com
Smoliak Dmitry Sergeevich